Bugs & Wish list
not able to authenticate user with e-Directory LDAP | Tiki Wiki CMS Groupware :: Development

not able to authenticate user with e-Directory LDAP

Status
● Open

Subject
not able to authenticate user with e-Directory LDAP

Version
4.x

Category
• Usability

Feature
External Authentication (LDAP, AD, PAM, CAS, etc)

Resolution status
New

Submitted by
talindoche

Lastmod by
talindoche

Rating
★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ (0) tableView

Description
Scenario:
TikiWiki version 4.1
Auth against LDAP
LDAP being used: Novell eDirectory

Problem:
user can not log in unless the complete DN of the user is specified.
In my scenario the users are spread across the complete tree, so no chance to provide a specific "User DN", additionally a "Base DN" needs to be specified in order restrict the search to the city where the service runs. Finally only the default option provided at the "LDAP Bind Type" seems to be correct for eDirectory.

How this has been solved:
1.- The code modified has been: lib/auth/ldap.php
2.- If the LDAP connect operation fails, then a try to search for the user is triggered
3.- If the user is found then the LDAP, the his/her DN is extracted and a new LDAP connect is performed.
Here the diff of the modified code:

diff -uN ldap.php ldap.php.new
@@ -200,6 +200,50 @@
 $this->ldaplink= Net_LDAP2::connect($options);
     if(Net_LDAP2::isError($this->ldaplink)) {
         /* This modification is placed in order to add a kind of e-Directory compatibility. 
+           For e-Directory and according to what I found about documentation - please consider I'm not an expert on this matter - 
+           e-Directory will only get a positive result for the user search (with is password) only if the dn is pointing to the place where 
+           the user object has been created, so we need first to find this data. 
+           In the next lines the user data will be searched, and once found (if found) the info related to binddn will be updated */
+         
+         // filters to locate the user
+         $filter1=Net_LDAP2_Filter::create('objectClass','equals',$this->options['useroc']);
+         $filter2=Net_LDAP2_Filter::create($this->options['userattr'],'equals',$this->options['username']);
+         $filter=Net_LDAP2_Filter::combine('and',array($filter1,$filter2));
+         if(Net_LDAP2::isError($filter)) {
+             $this->add_log('ldap','LDAP Filter creation error: '.$filter->getMessage().' at line '.__LINE__.' in '.__FILE__);
+             return false;
+         }
+         $searchoptions=array('scope' => $this->options['scope']);
+         // unset the binddn, if set then the connect will fail
+         unset ($options['binddn']);
+         $this->ldaplink= Net_LDAP2::connect($options);
+         if(Net_LDAP2::isError($this->ldaplink)) {
+             $this->add_log('ldap','Error: '.$this->ldaplink->getMessage().' at line '.__LINE__.' in '.__FILE__);
+             return($this->ldaplink->getCode());
+         }
+         $searchresult =
+         $this->ldaplink->search($this->options['basedn'],$filter,$searchoptions);
+         if($searchresult->count()!=1) {
+             // More then 1 user ... problem
+             $this->add_log('ldap','Error: ldap search found this amount of useres: '.$searchresult->count().' which is not 1. at line '.__LINE__.' in '.__FILE__);
+             return false;
+         }
+         $entry=$searchresult->shiftEntry();
+         if (Net_LDAP2::isError($entry)) {
+             $this->add_log('ldap','Error fetching user entries: '.$entry->getMessage().' at line '.__LINE__.' in '.__FILE__); 
+         }
+         $searchoptions=array('scope' => $this->options['scope']);
+         // unset the binddn, if set then the connect will fail
+         unset ($options['binddn']);
+         $this->ldaplink= Net_LDAP2::connect($options);
+         if(Net_LDAP2::isError($this->ldaplink)) {
+             $this->add_log('ldap','Error: '.$this->ldaplink->getMessage().' at line '.__LINE__.' in '.__FILE__);
+             return false;
+         }
+         $searchresult =
+         $this->ldaplink->search($this->options['basedn'],$filter,$searchoptions);
+         if($searchresult->count()!=1) {
+             // More then 1 user ... problem
+             $this->add_log('ldap','Error: ldap search found this amount of useres: '.$searchresult->count().' which is not 1. at line '.__LINE__.' in '.__FILE__);
+             return false;
+         }
+         $entry=$searchresult->shiftEntry();
+         if (Net_LDAP2::isError($entry)) {
+             $this->add_log('ldap','Error fetching user entries: '.$entry->getMessage().' at line '.__LINE__.' in '.__FILE__); 
+         }
References:
Info in TikiForum
Info about eDirectory

Hope this could be a kind of contribution
TalindoChe

Importance
1 low
Priority
5

Demonstrate Bug
Please demonstrate your bug on show2.tikiwiki.org

Version: trunk ▼ Create show2.tikiwiki.org instance

Ticket ID
2973

Created
Wednesday 13 January, 2010 22:33:28 GMT-0000

LastModif
Wednesday 13 January, 2010 22:33:28 GMT-0000
The original document is available at
http://dev.tiki.org/item2973-not-able-to-authenticate-user-with-e-Directory-LDAP